論文賞受賞研究
「匿名通信のための情報量的に安全な暗号化/認証技術」
「鍵漏洩耐性をもつ不正利用者追跡法」

2008.05.16
花岡 悟一郎
RCIS, AIST

はじめに

- 発表者の研究の大きな目的:「高度に安全」な暗号技術の追求
  …「高度に安全」とは？
  - 数学的仮定の排除（実現可能性重視）
  - より弱い数学的仮定（実用性重視）
  - 秘密情報の漏洩への耐性

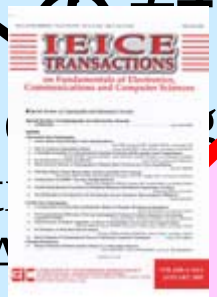
最近の成果の例

- 数学的仮定の排除
  - Unconditionally Secure A
    Group Authentication. ***Comput.***
    200
- 「印象に残った論文」仮定
  - 選択暗号文攻撃に対して証明可能
    . **SCIS'08**予稿集, 2008.
- 秘密情報の漏洩への耐性
  - Traitor Tracing Scheme S
    Exposure and its Applicat
    IEICE Transactions 90-A

The Wilkes Award
from
British Comp. Society

ISEC
Information Security

「印象に残った論文」
from
SCIS'08（非公式）

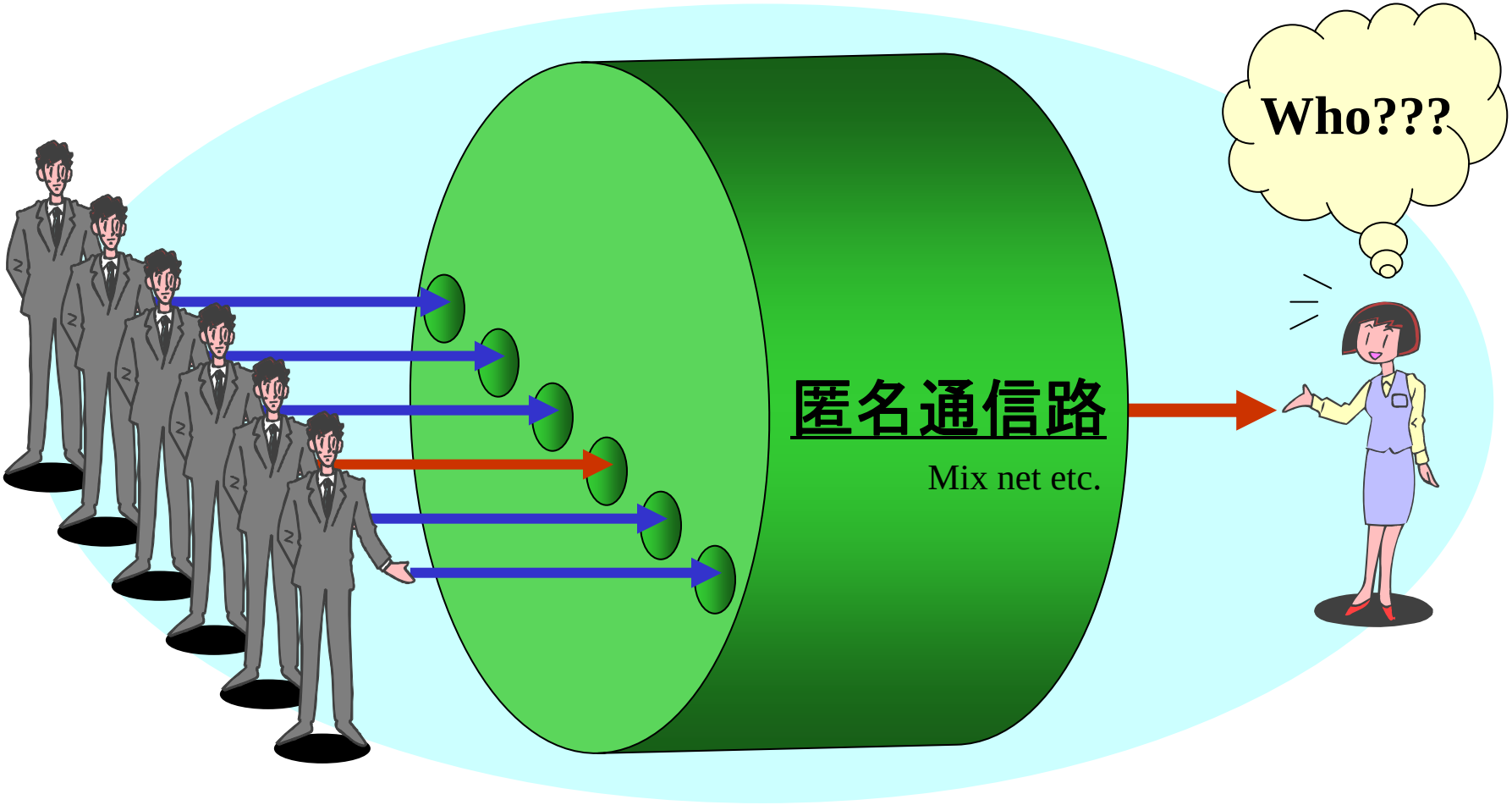


Best Paper Award
from
IEICE

「匿名通信のための情報量的に安全な暗号化/認証技術」

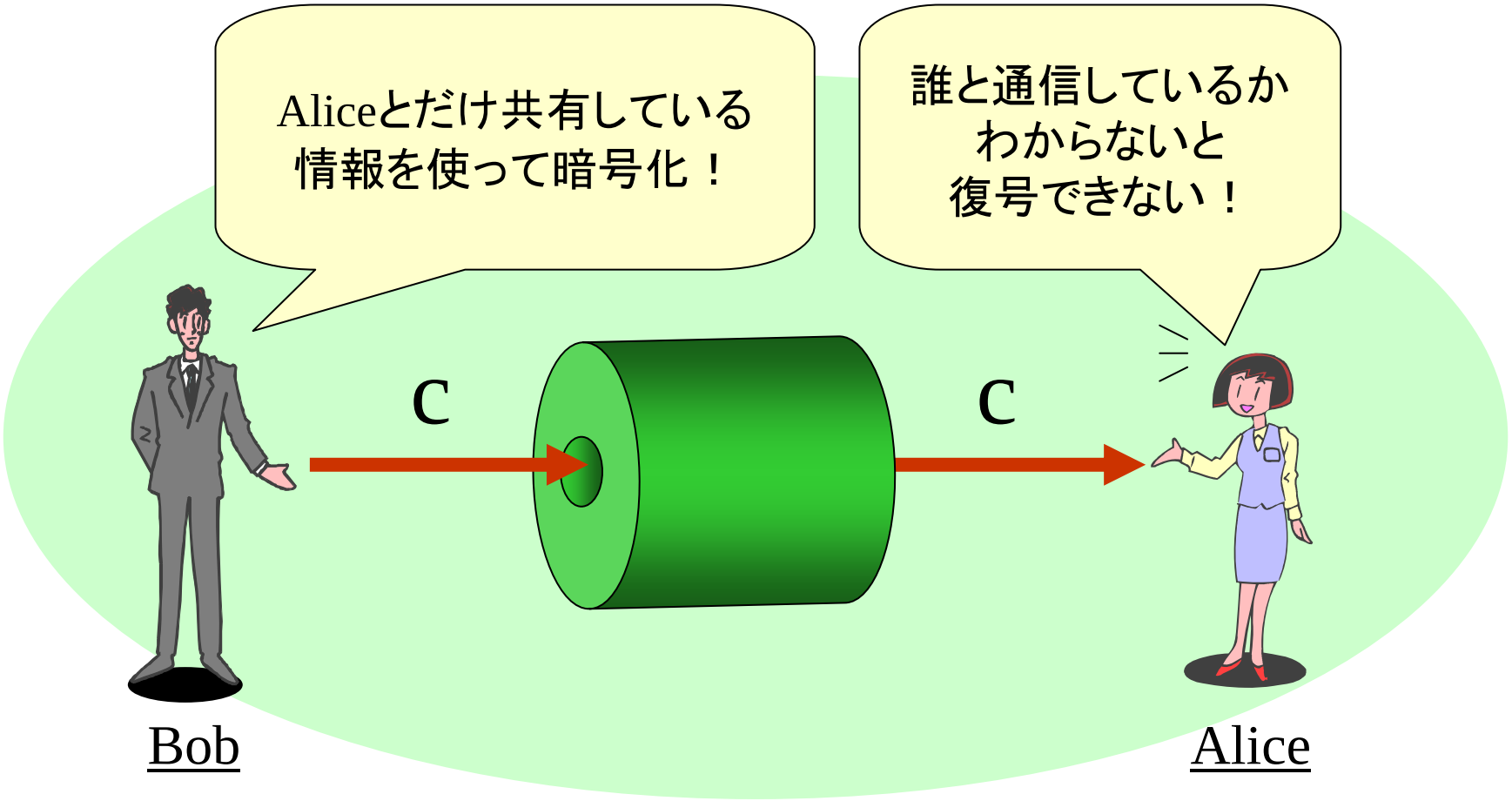
- Unconditionally Secure Anonymous Encryption and Group Authentication. Hanaoka, Shikata, Imai. ***Comput. J***. 49(3): 310-321, 2006.
- 匿名通信における、無条件に安全な秘匿/認証通信の理論的限界の解明と最適な実現方法の提示
- British Computer Society（英国）より、***The Wilkes Award***（2006）を受賞
  - 学術論文誌 *The Computer Journal* に掲載論文のうち、年間を通じて一件のみに授与される。

匿名通信路



匿名通信と情報量的安全性

匿名通信と情報量的安全性は両立が難しい！



この研究の成果

- 匿名通信と情報量的安全性を両立させるための条件を明確にした。
  - 鍵長, 暗号文長, etc…
- 実際に、この要件を満足する、最適な方式の存在を示した。

The Computer Journal

http://comjnl.oxfordjournals.org/

Maurice Wilkes

nt changes
ct Wikipedia
te to Wikipedia

Search

links here
ed changes
d file
al pages
ble version
anent link
his page

sch
ñol
ais

lands

guês

Sir Maurice Vincent Wilkes FRS (born June 26, 1913 in Dudley, Staffordshire, England) is a British computer scientist, credited with several important developments in computing.

Wilkes studied at St. John's College, Cambridge from 1931 to 1934, continuing to complete a Ph.D. in physics, on the topic of radio propagation of very long radio waves in the ionosphere in 1936. He was appointed to a junior faculty position of the University of Cambridge through which he was involved in the establishment of a computing laboratory.

Wilkes was called up for military service during WWII and worked on radar at the Telecommunications Research Establishment (TRE), and in operational research.

In 1945, he was appointed as the second director of the University of Cambridge Mathematical Laboratory (later known as the Computer Laboratory).

The Cambridge laboratory initially had many different computing devices, including a differential analyser. Wilkes obtained a copy of John von Neumann's prepress description of the

Maurice Vincent Wilkes

Born	June 26, 1913 (age 94) Dudley, Staffordshire
Nationality	British
Fields	Computer Science
Institutions	Telecommunications Research Establishment University of Cambridge Mathematical Laboratory British Computer Society Digital Equipment Corporation
Known for	Microprogramming
Notable awards	Turing Award

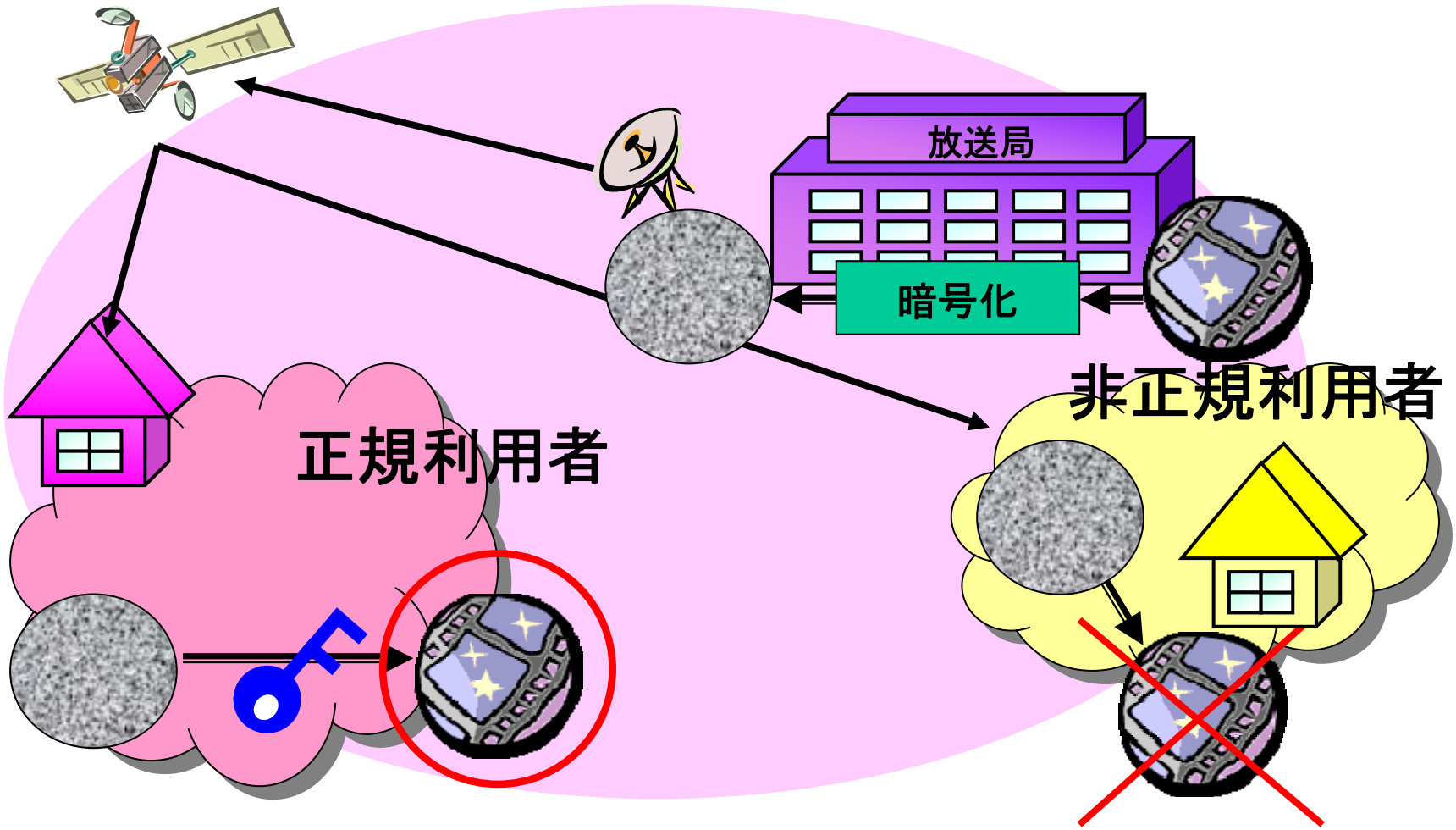
⋮

Wikipediaより引用

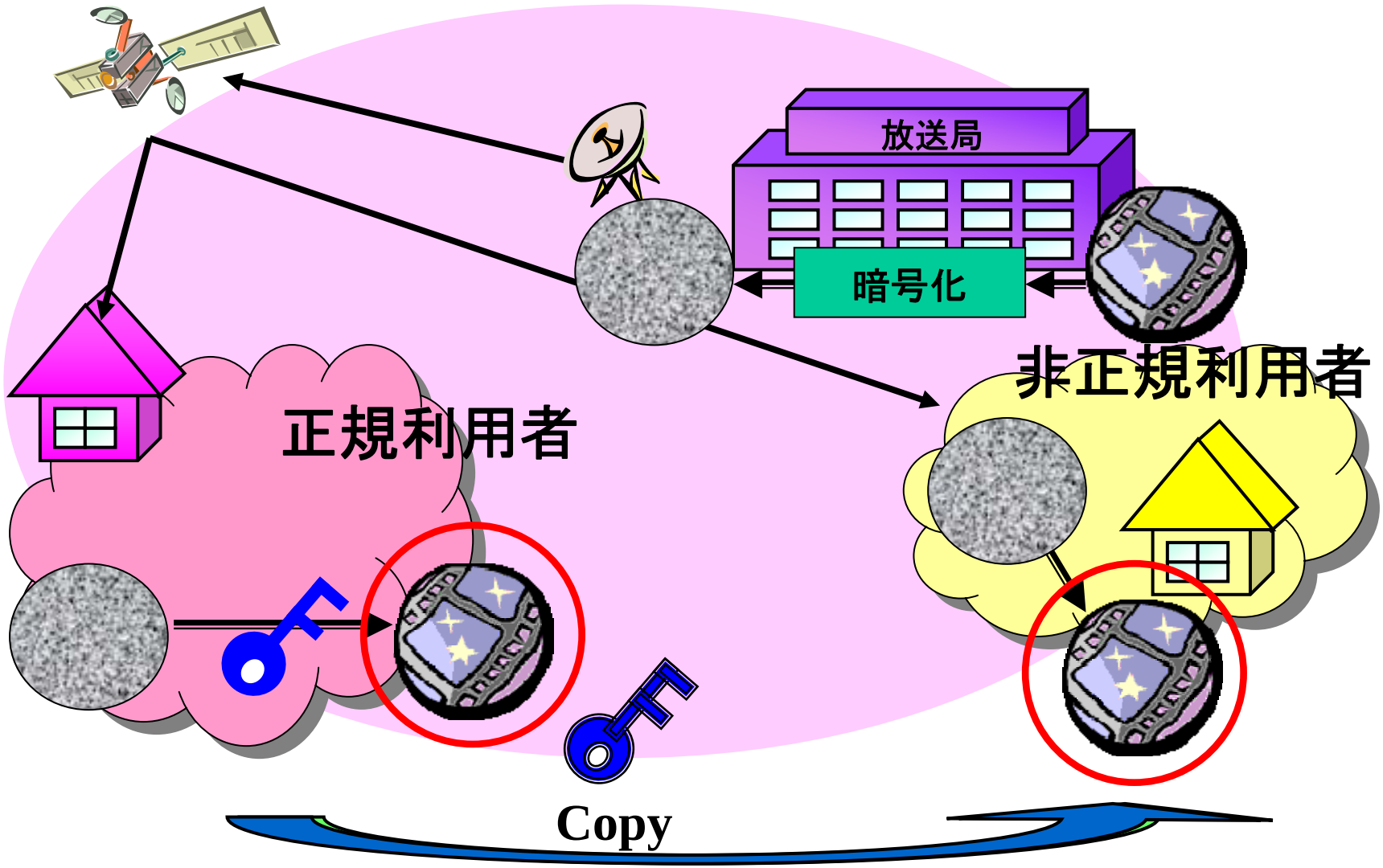
「鍵漏洩耐性をもつ不正利用者追跡法」

- Traitor Tracing Scheme Secure against Adaptive Key Exposure and its Application to Anywhere TV Service. Ogawa, Hanaoka, Imai. ***IEICE Transactions*** 90-A(5): 1000-1011, 2007.
- 有料放送通信における、復号鍵の不正な二次配布者の追跡可能性と、秘密情報漏洩への耐性を同時に実現
- 電子情報通信学会（日本）より、***平成19年度論文賞***を受賞
  - 学術論文誌 *IEICE Trans. Fundamentals* に掲載論文のうち、年間を通じて三件のみに授与される。

有料放送通信



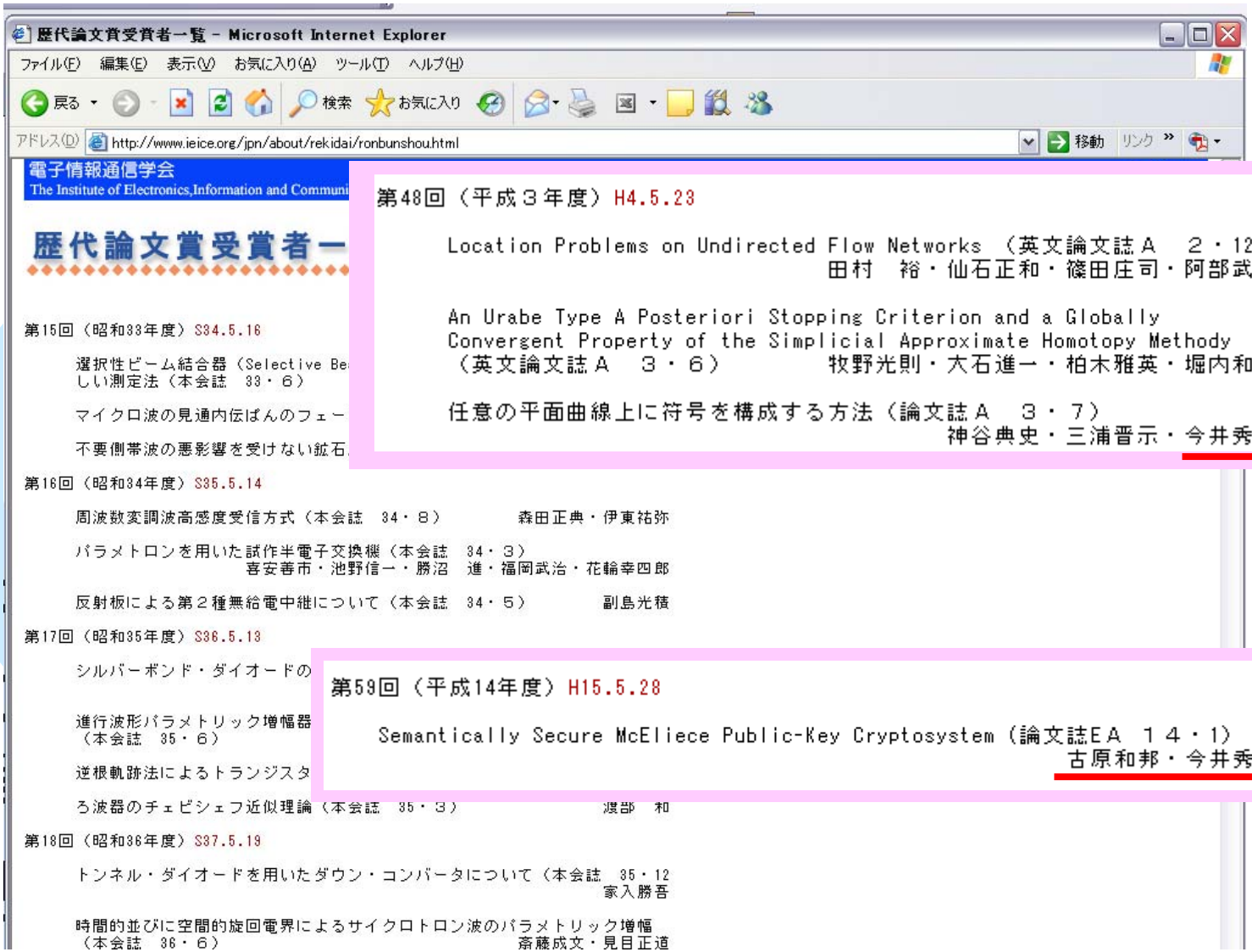
不正な二次配布者の存在もしくは不注意による鍵漏洩の問題



この研究の成果

- 次の二つの性質を満たす有料放送通信のための暗号方式の提案
  - 不正に二次配布された鍵から、その漏洩元となった利用者を特定可能。
  - ある時点における鍵情報が漏洩しても、それ以降における安全性は損なわれない。

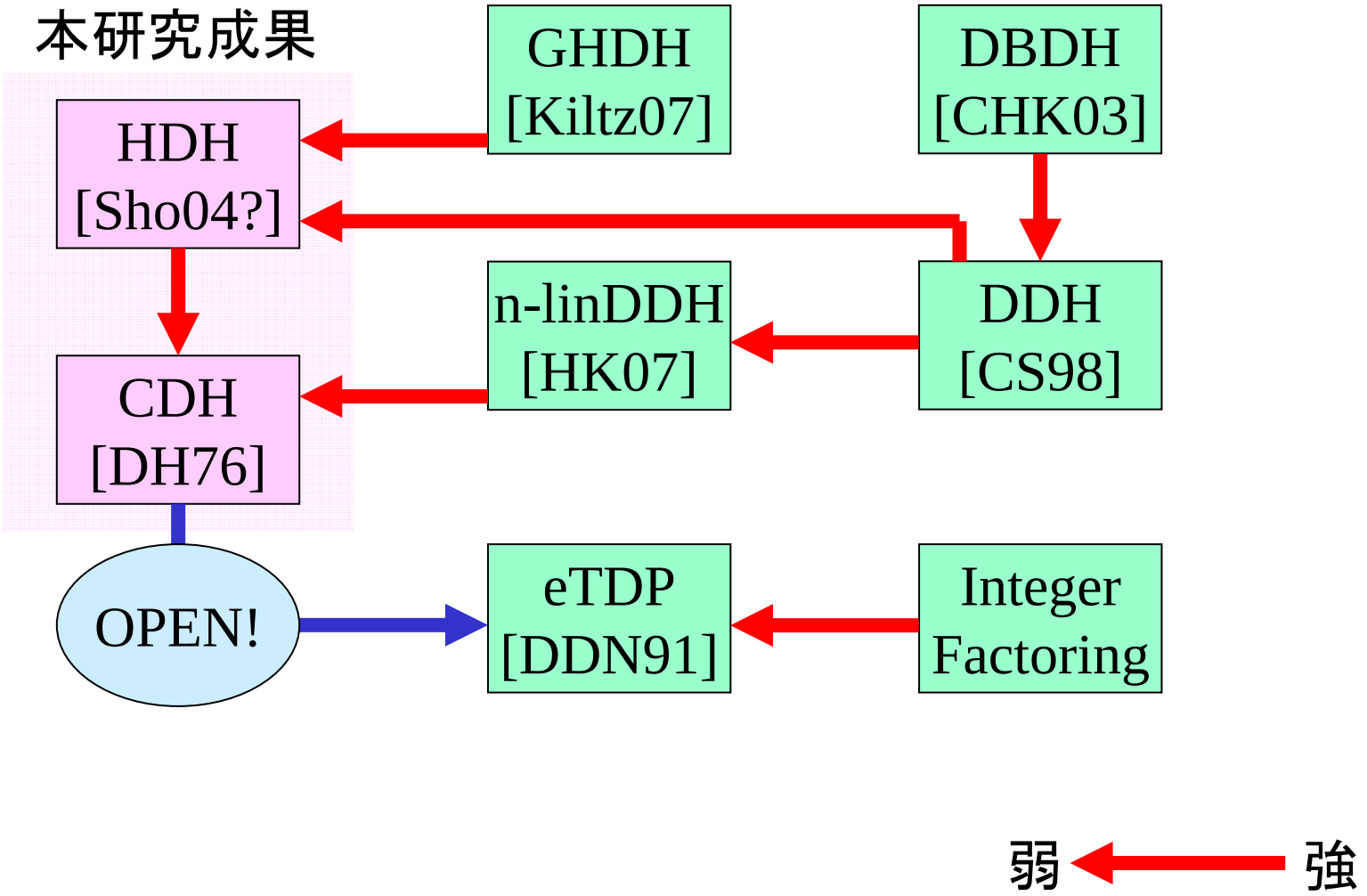
過去の信学会論文賞受賞者



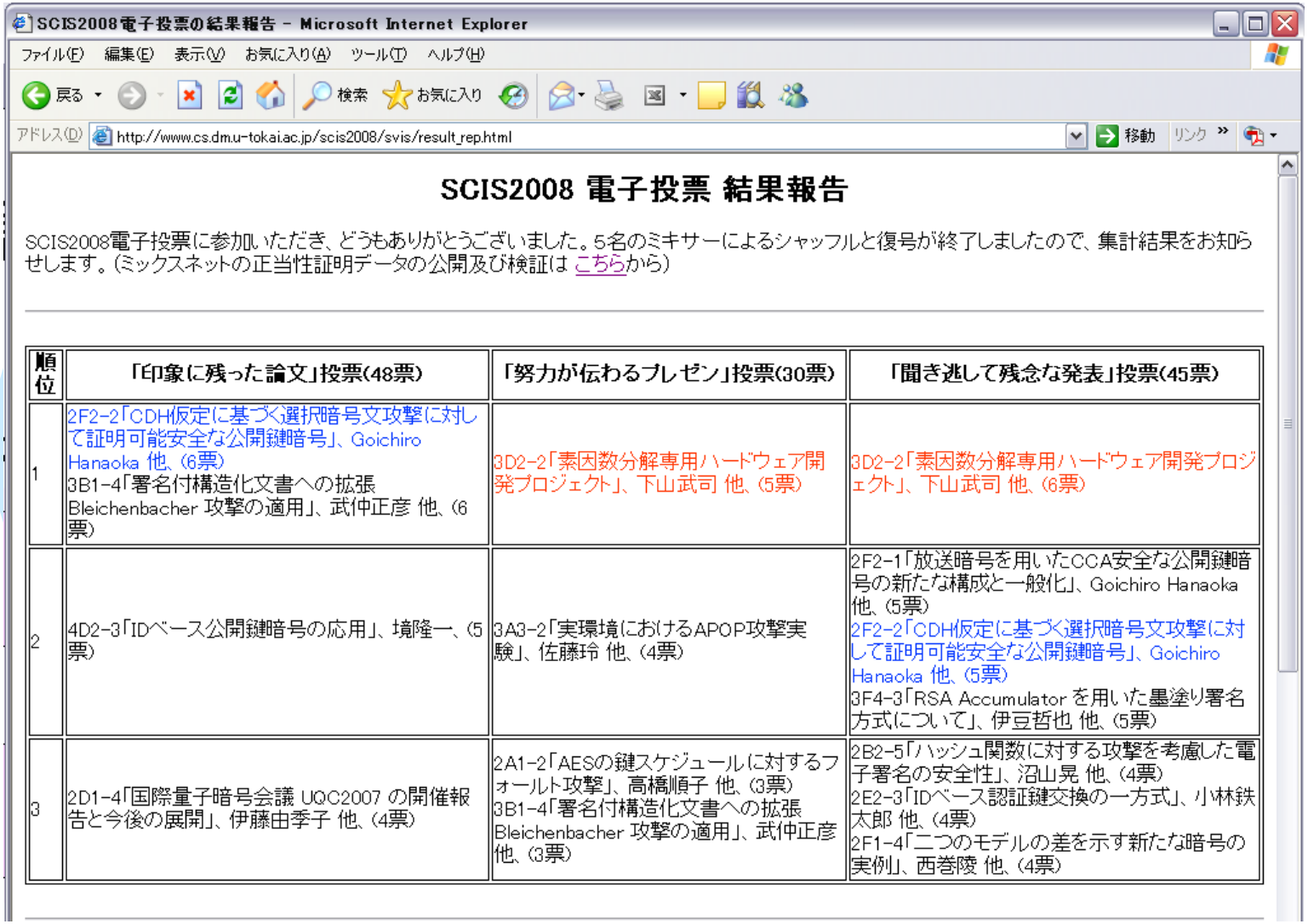
「CDH仮定に基づく選択暗号文攻撃に対して証明可能安全な公開鍵暗号」

- CDH仮定に基づく選択暗号文攻撃に対して証明可能安全な公開鍵暗号. Hanaoka, Imai. SCIS'08 予稿集, 2008.
- 従来の方式よりも弱い仮定のみを用いて、選択暗号文攻撃への安全性を証明可能な公開鍵暗号方式を提案
- 国内研究会SCIS'08において、「印象に残った論文」部門（非公式 ☺） 第一位に選ばれる。
  - 「聞き逃して残念な発表」部門でも第二位に選出。

簡単な背景: CCA安全性の仮定



SCIS2008投票結果



SCIS2008 電子投票 結果報告

SCIS2008電子投票に参加いただき、どうもありがとうございました。5名のミキサーによるシャッフルと復号が終了しましたので、集計結果をお知らせします。(ミックスネットの正当性証明データの公開及び検証は こちらから)

順位	「印象に残った論文」投票(48票)	「努力が伝わるプレゼン」投票(30票)	「聞き逃して残念な発表」投票(45票)
1	2F2-2「CDH仮定に基づく選択暗号文攻撃に対して証明可能安全な公開鍵暗号」、Goichiro Hanaoka 他、(6票) 3B1-4「署名付構造化文書への拡張 Bleichenbacher 攻撃の適用」、武仲正彦 他、(6票)	3D2-2「素因数分解専用ハードウェア開発プロジェクト」、下山武司 他、(5票)	3D2-2「素因数分解専用ハードウェア開発プロジェクト」、下山武司 他、(6票)
2	4D2-3「IDベース公開鍵暗号の応用」、境隆一、(5票)	3A3-2「実環境におけるAPOP攻撃実験」、佐藤玲 他、(4票)	2F2-1「放送暗号を用いたCCA安全な公開鍵暗号の新たな構成と一般化」、Goichiro Hanaoka 他、(5票) 2F2-2「CDH仮定に基づく選択暗号文攻撃に対して証明可能安全な公開鍵暗号」、Goichiro Hanaoka 他、(5票) 3F4-3「RSA Accumulator を用いた墨塗り署名方式について」、伊豆哲也 他、(5票)
3	2D1-4「国際量子暗号会議 UQC2007 の開催報告と今後の展開」、伊藤由季子 他、(4票)	2A1-2「AESの鍵スケジュールに対するフォールト攻撃」、高橋順子 他、(3票) 3B1-4「署名付構造化文書への拡張 Bleichenbacher 攻撃の適用」、武仲正彦 他、(3票)	2B2-5「ハッシュ関数に対する攻撃を考慮した電子署名の安全性」、沼山晃 他、(4票) 2E2-3「IDベース認証鍵交換の一方式」、小林鉄太郎 他、(4票) 2F1-4「二つのモデルの差を示す新たな暗号の実例」、西巻陵 他、(4票)